UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

Evidence Item #1: One black Apple iPhone XR, IMEI: 356448100722900, in a black case, currently in the custody of the St. Louis County Police Department, 7900 Forsyth Blvd., Clayton, MO 63105, within the Eastern District of Missouri

4:21 MJ 5268 NAB
FILED UNDER SEAL

) SIGNED AND SUBMITTED TO THE COURT FOR
) FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Stephanie Stoehner, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the Eastern District of Missouri, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- xx evidence of a crime;
- xx contraband, fruits of crime, or other items illegally possessed;
- xx property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title Section	
Title 18, United States Code, Sections 2252A	receipt and shipment of child pornography, and other related materials

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ✓ Continued on the attached sheet.
- ❑ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

DET. STOEHNER 3932
Applicant's signature
Stephanie Stoehner, TFO, FBI
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 09/ 15 /2021

Judge's signature

City and State: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge
Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF **Evidence Item #1: One black Apple iPhone XR, IMEI: 356448100722900, in a black case, currently in the custody of the St. Louis County Police Department, 7900 Forsyth Blvd., Clayton, MO 63105, within the Eastern District of Missouri**	)	No. 4:21 MJ 5268 NAB
	)	FILED UNDER SEAL
	)	SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Stephanie Stoehner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am presently a Task Force Agent with the Federal Bureau of Investigation and a Detective assigned to the St. Louis County Police Department Division of Criminal Investigation's Special Investigations Unit where I conduct investigations into state and federal offenses involving child pornography, human trafficking, child sexual abuse and internet-facilitated crimes against children among other offenses. I have been a police officer for approximately 11 years. During my time as a law enforcement officer, I have utilized a variety of investigative techniques to include: organizing and participating in physical surveillance; participating in undercover operations; serving search warrants; making arrests; and interviews involving defendants. As part of my duties as a Detective/Task Force Officer, I investigate

crimes involving violation of Title 18, United States Code, Sections 2252A (possession, receipt and distribution of child pornography). I have received specialized training in the area of child pornography offenses and internet-facilitated crimes against children.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §2252A, Receiving/Distributing Child Pornography, have been committed by Nicholas Haglof. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is: Evidence Item #1: one black Apple iPhone XR, IMEI 356448100722900 in a black case (hereinafter "the Device"). The Device is currently located at St. Louis County Police Department, 7900 Forsyth Blvd, Clayton, MO 63105**.** The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

and internet activity through radio signals, wi-fi and bluetooth. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Wireless telephone

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet,

connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

7. Based on my training, experience and research, I know that the Device has capabilities that allows it to serve as a wireless telephone, digital camera, computer, internet browser, digital communicator, portable media player, GPS navigation device, and PDA**.** In my training and experience, examining data stored on such devices can uncover, among other things, evidence that reveals or suggests who possessed or used the Device, how the Device was used, and details regarding communications utilizing the Device and activities undertaken utilizing the Device.

PROBABLE CAUSE

8. On July 27, 2020, Sergeant Adam Kavanaugh, DSN 2877, of the St. Louis County Police Department's Special Investigations Unit, advised me that CyberTipline Report #5918831 from the National Center for Missing and Exploited Children (NCMEC) had been forwarded to the Special Investigations Unit.

9. CyberTipline Report #59188301, which was reported to NCMEC on November 12, 2019 at 02:21:23 hours (UTC) by Microsoft Online Operations, in reference to the "Bing Image" web-based search engine. Per CyberTipline Report #59188301, between November 10, 2019 at 00:27:11 hours (UTC) and November 10, 2019 at 00:28:53 hours (UTC), an unknown user utilizing a device and/or devices with the Internet Protocol (IP) address 2600:6c40:4200:3abf:95df:1968:47a4:76d4 had either possessed or attempted to possess files of suspected child pornography. CyberTipline Report #59188301 indicated that a representative Microsoft Online Operations reviewed the 7 image files, including the following file:

FILE NAME: 4203f315-b651-4a62-8a82-a52942ce0736.jpg

DESCRIPTION: An image file depicting a prepubescent female wearing red/black thigh-high tights positioned on her knees and bent at the waist with her legs spread apart, making her vagina and anus the focal point of the image.

10. I conducted an inquiry of law enforcement databases, and discovered that on October 20, 2018, Allison Lehmkuhl married Nicholas Haglof. The inquiry further indicated that Allison Haglof and Nicholas Haglof moved into the home of Allison Haglof's parents (James and Cherryl Lehmkuhl), located at 563 Goldwood Dr., Ballwin, MO 63021 in June 2020, and subsequently purchased the residence located at 331 Turfwood Dr., Ballwin, MO 63021 in July 2020.

11. On July 31, 2020, Detective Amy Meyer, DSN 3444, of the St. Louis County Police Department's Special Investigations Unit, contacted Allison Haglof at 563 Goldwood Dr., Ballwin, MO 63021. Allison Haglof informed Detective Meyer that she and her husband Nicholas Haglof, did possess multiple laptop computers which had been moved from their previous residence of 1448 Brookside Dr., High Ridge, MO 63049 to 563 Goldwood Dr., Ballwin, MO 63021. Detective Meyer observed approximately 3 laptops in the home located at 563 Goldwood Dr., Ballwin, MO 63021.

12. On July 31, 2020, I seized the Device from Nicholas Haglof at the Maryland Heights Police Department and examined its exterior. The Device did not have any indications of the Device's model number, serial number, or IMEI number. I packaged the Device as Evidence Item #1.

13. The Device was searched pursuant to a previous search warrant signed on July 31, 2020 by St. Louis County, Missouri Circuit Judge Michael Burton, authorizing a search of the Device which was seized from Nicholas Haglof in Maryland Heights, Missouri, for, *inter alia*, an electronic device that was believed to contain evidence of child pornography offenses.

14. The search warrant was executed by Detective Michael Slaughter, DSN 3562, of the St. Louis County Police Department's Special Investigations Unit on August 3, 2020. Detective Slaughter's performed an advanced logical extraction of the Device using a forensic tool called Cellebrite UFED TOUCH2-7211803 produced by Cellebrite Mobile Synchronization, Ltd.

15. Detective Slaughter and I reviewed the examination of the Device using Cellebrite's Physical Analyzer (hereinafter "PA"). During the review of the extracted data, it was determined that the Device was named "Nick's Device" and was assigned IMEI: 356448100722900. The Device was not found to contain suspected child pornography in the 2020 forensic examination. However, substantial advances in the forensic tools available to examine such devices have been made, raising the possibility that reexamination would yield relevant evidence of Nicholas Haglof's possession, receipt and distribution of child pornography. Detective Slaughter created a web report in Cellebrite's PA of the forensic exam of the Device, which he saved to a disc and packaged as Evidence Item #FE-1.

16. A subsequent review of Evidence Item #FE-1 revealed that the web report was incomplete.

17. The Device has remained in the custody of law enforcement since July 31, 2020, and has been secured, stored and preserved in a manner such that it, to the extent material to this investigation, is likely to retain much of the data it contained at the time it was seized.

Meanwhile, since 2020, there have been advancements in the tools available for forensic analysis of mobile devices that allow analysts to recover more evidence from a mobile device than previously possible.

18. An indictment of Nicholas Haglof for receipt of child pornography in violation of 18 U.S.C. §2252A was returned on or about August 1, 2020, in case no. 4:20 MJ 5152-NAB. This case is presently pending.

19. Based on my experience and training, individuals who engage in criminal activity involving child pornography and internet-facilitated crime against children, including violation of 18 U.S.C. §2252A, often utilize text messaging, social media, the internet, chat rooms and other tools available on mobile devices to receive, distribute and view child pornography, to search for child pornography, to communicate with others regarding child pornography or child sexual abuse and to meet, groom and communicate with children in a manner relevant to criminal activity.

20. Based on the foregoing, I believe there is probable cause to conclude that Nicholas Haglof utilized the Device to further his violation of child pornography laws; that the Device contains evidence of child pornography and internet-facilitated crimes against children; and that new forensic tools that were not available in 2020 will allow a more thorough and accurate examination of the Device. The Device is currently in the lawful possession of the St. Louis County Police Department**.** Therefore, while the investigative agency might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, activity over the internet; images that have been saved, received, sent or viewed; and digital communications are typically stored for some period of time on mobile electronic devices. This information can be recovered with forensics tools.

22. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

THE REMAINDER OF THIS PAGE LEFT INTENTIONALLY BLANK

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

25. Because this warrant seeks only permission to examine Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

I state under the penalty of perjury that the foregoing is true and correct.

09/15/2021
DATE

DET. STOENER 3932
STEPHANIE STOEHNER
TFO
Federal Bureau of Investigation (FBI)

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on the 15th day of September, 2021.

HONORABLE NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE
Eastern District of Missouri

ATTACHMENT A

Evidence Item #1: One Black Apple iPhone XR, IMEI: 356448100722900 in a black case, Currently in the Custody of the St. Louis County Police Department, 7900 Forsyth Blvd. Clayton, MO, 63105, within the Eastern District of Missouri.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records, information and data on the that relate to violations of 18 U.S.C. 2252A, possession, receipt and distribution of child pornography, and involve Nicholas Haglof, including any communications, images, videos, depictions, audio-files, records or information of a sexual nature related to any minor(s) and any communications and any images, videos, depictions, audio-files, records related to Nicholas Haglof's searches for child pornography and child erotica; his possession, receipt, distribution and viewing of child pornography and child erotica; and communications and contacts related to his interest in child pornography, child erotica and a sexual interest in minors.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, viewed, received, sent, such as logs, phonebooks, saved usernames and passwords, documents, internet activity, electronic activity and browsing history;

3. Evidence of the state of mind of Nicholas Haglof or others relative to communications, images, videos, depictions, audio-files, records, internet activity, social media activity or information related to child pornography, child erotica and internet-facilitated crimes against children.